WHAT ARE THE LAST DIGITS OF ...?

EDWARD OMEY AND STEFAN VAN GULCK

Abstract. We propose a class assignment where students are asked to construct and implement an efficient algorithm to calculate the last digits of a positive integral power of a positive integer. The mathematical prerequisites for this assignment are very limited: knowledge of remainder calculus and the binary representation of a positive integer. The periodicity of the last digits is studied by means of the Euler totient function and the Carmichael function.

1. Introduction

As an exercise, students are sometimes asked to find the last digit of, for example, 7^{9999}; see [1, 2, 3, 4] for such and related, more difficult questions. For this and many other cases, it is often easy to find the last digit: calculate some powers and detect a cyclical pattern. Table 1 shows that the last digit of 7^x takes the values 7, 9, 3, and 1 for powers of the form $x = 4k+1$, $4k+2$, $4k+3$, and $4k+4$, respectively, with $k \in \mathbb{N}_0 = \{0, 1, 2, \ldots\}$. Since $9999 = 4 \times 2499 + 3$, we find that the last digit of 7^{9999} is 3.

Table 1. Last digit of the first 7 powers of 7.

x	7^x	last digit
1	7	7
2	49	9
3	343	3
4	2401	1
5	16807	7
6	117649	9
7	823543	3

Table 1 also reveals that the last two digits of 7^x exhibit the same cyclical pattern. Therefore, as a bonus, we discover that the last two digits of 7^{9999} are given by 43.

The situation becomes more complicated when we want to find, for example, the last 5 digits of 7^{9999}. From the practical point of view, it is not possible to calculate enough powers of 7 to find a cyclical pattern for the last 5 digits.

This paper describes an algorithm to find the last m digits of y^x, where $m, x, y \in \mathbb{N} = \{1, 2, \ldots\}$. Our strategy will consist of replacing x by its binary representation and to find the remainders of the division of y^{2^n} by $z = 10^m$ for all powers 2^n that appear in the binary representation of x. This algorithm is likely known to students who have followed a course in Number Theory [5, 6, 7], but its beauty can be

Key words and phrases. class assignment; last digits; binary representation; remainder of division; recursive solution; cycle length; Euler totient function; Carmichael function.

appealing to other students and motivate them to delve into the study of this interesting mathematical sub-discipline. Ideally, this assignment is supplemented with a discussion of applications to the fields of Cryptography [5, 6, 7] and Stochastic Simulation [8, 9].

The construction and implementation of the algorithm can be the content of a class assignment, with sufficient guidance by the teacher. The only mathematical prerequisites are some elementary arithmetic rules. The benefit of such an assignment is that it can be motivating for students to experience how their (limited) knowledge of mathematics (binary representation and remainder calculus) can be combined in order to solve a seemingly hard problem.

Table 1 shows the periodic behaviour of the last (two) digit(s) of y^x in case $y = 7$. In the last section, we study the periodicity of the last m digits of y^x. The period is bounded above by Euler's totient function, which is well known in Number Theory [5, 6, 7, 10, 11]. This upper bound is improved by using Carmichael's function [12, 11], a function that is seldom discussed in an introductory course in Number Theory. For example, it is absent in [5, 6, 7]. Neither have we found a paper in the present journal where Carmichael's function appears.

2. Binary expansion

The binary representation of x is

$$x = \sum_{i=0}^{\infty} a_i 2^i, \tag{2.1}$$

where $\{a_i\}_{i\in\mathbb{N}_0} \in \{0,1\}^{\mathbb{N}_0}$. The number of non-zero terms in (2.1) is finite, where the largest non-zero coefficient a_i has index $i = n$ satisfying $2^n \le x < 2^{n+1}$, i.e. $n = \lfloor \log_2 x \rfloor$.

In order to recursively determine the coefficients $\{a_i\}_{i\in\mathbb{N}_0}$ in (2.1), we define a non-increasing sequence $\{x_n\}_{n\in\mathbb{N}_0}$ of non-negative integers, with a finite number of non-zero terms, by

$$x_n = \sum_{i=n}^{\infty} a_i 2^{i-n}. \tag{2.2}$$

From (2.2) follows that

$$a_n = \begin{cases} 1 & \text{if } x_n \text{ is odd,} \\ 0 & \text{if } x_n \text{ is even.} \end{cases} \tag{2.3}$$

In both cases of (2.3), it holds that

$$x_{n+1} = \sum_{i=n+1}^{\infty} a_i 2^{i-(n+1)} = \frac{x_n - a_n}{2} = \left\lfloor \frac{x_n}{2} \right\rfloor. \tag{2.4}$$

Formulae (2.3) and (2.4) can recursively be applied in order to determine the binary expansion (2.1) according to the following algorithm:

1. Let $n = 0$, $x_0 = x$, $a_0 = 0$ if x_0 is even, $a_0 = 1$ if x_0 is odd, and go to step 2.
2. If $n = \lfloor \log_2 x \rfloor$, then display $(a_0, \ldots, a_n)$; otherwise go to step 3.
3. Let $n = n + 1$, $x_n = \lfloor x_{n-1}/2 \rfloor$, $a_n = 0$ if x_n is even, $a_n = 1$ if x_n is odd, and return to step 2.

For example, for $x = 54$ we find $54 = 2 + 2^2 + 2^4 + 2^5$; see Table 2.

Table 2. Determination of the binary representation of 54.

n	x_n	a_n
0	54	0
1	27	1
2	13	1
3	6	0
4	3	1
5	1	1

3. Remainder of a division

The last $m = 2$ digits of the number $y = 12345$ are given by 45. Another way to express this is $12345 = 45 + 123 \times 100$. The number 45 is the remainder of $y = 12345$ after dividing y by $z = 100$. We write $45 = 12345 \bmod 100$.

More generally, for $z \in \mathbb{N}$ and $a \in \{0, \ldots, z-1\}$, the notation $a = y \bmod z$ means that there exists a unique $k \in \mathbb{N}_0$ such that $y = a + kz$. Alternatively, $y \bmod z = z(y/z - \lfloor y/z \rfloor)$. The use of modulo-calculus is very elegant and useful in solving our problem.[1]

If $a = x \bmod z$ and $b = y \bmod z$, then there exists $k, l \in \mathbb{N}_0$ such that $x = a + kz$ and $y = b + lz$. Hence, $xy = ab + (al + bk + klz)z$. If $c \in \mathbb{N}_0$ satisfies $ab = (ab) \bmod z + cz$, then $(xy) = (ab) \bmod z + dz$ with $d = c + al + bk + klz \in \mathbb{N}_0$. We can therefore conclude that

$$(xy) \bmod z = (ab) \bmod z \qquad \text{if} \qquad \begin{cases} a = x \bmod z, \\ b = y \bmod z. \end{cases} \tag{3.1}$$

In order to use the binary representation (2.1), we introduce the notation $b_n = y^{2^n} \bmod z$. Combining (2.1) and (3.1) yields

$$y^x \bmod z = \left(\prod_{n=0}^{\infty} y^{a_n 2^n} \right) \bmod z = \left(\prod_{n=0}^{\infty} b_n^{a_n} \right) \bmod z. \tag{3.2}$$

Since $y^{2^{n+1}} = \left(y^{2^n}\right)^2$, a second application of (3.1) gives

$$b_{n+1} = b_n^2 \bmod z. \tag{3.3}$$

Hence, the sequence $\{b_n\}_{n \in \mathbb{N}_0}$ can recursively be determined, which avoids the calculation of too large powers of y.

4. Algorithm

In order to recursively calculate $y^x \bmod z$ in (3.2), we use the following notation:

$$c_n = \left(\prod_{i=0}^{n} b_i^{a_i} \right) \bmod z. \tag{4.1}$$

[1] Our notation deviates from the usual notation $x \equiv y \pmod z$ from Number Theory, see e.g. [5], with $x, y \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ and $z \in \mathbb{N}$, and which means that $z \mid x - y$, i.e. there exists a $k \in \mathbb{Z}$ such that $x - y = kz$ (in words: z is a divisor of $x - y$).

A third application of (3.1) now gives $c_{n+1} = \left(c_n b_{n+1}^{a_{n+1}}\right) \bmod z$, i.e.

$$c_{n+1} = \begin{cases} c_n & \text{if } a_{n+1} = 0, \\ (c_n b_{n+1}) \bmod z & \text{if } a_{n+1} = 1. \end{cases} \tag{4.2}$$

The algorithm is based on (2.4), (2.3), (3.3), and (4.2), and is an extension of the algorithm in section 2.

1. Let $n = 0$, $x_0 = x$, $a_0 = 0$ if x_0 is even, $a_0 = 1$ if x_0 is odd, $b_0 = y \bmod z$, and $c_0 = b_0^{a_0}$.
2. If $n = \lfloor \log_2 x \rfloor$, then output $y^x \bmod z = c_n$; otherwise go to step 3.
3. Let $n = n + 1$, $x_n = \lfloor x_{n-1}/2 \rfloor$, $a_n = 0$ if x_n is even, $a_n = 1$ if x_n is odd, $b_n = b_{n-1}^2 \bmod z$, $c_n = (c_{n-1} b_n^{a_n}) \bmod z$, and return to step 2.

Table 3 illustrates the algorithm and shows that the last five digits of 2014^{2013} are given by 30144. Of course, the algorithm is not restricted to cases where $z = 10^m$. The reader can now verify that $654^{987} \bmod 123 = 36$.

Table 3. Calculation of the last five digits of 2014^{2013}.

n	x_n	a_n	b_n	c_n
0	2013	1	02014	02014
1	1006	0	56196	02014
2	503	1	90416	97824
3	251	1	53056	50144
4	125	1	39136	35584
5	62	0	26496	35584
6	31	1	38016	61344
7	15	1	16256	08064
8	7	1	57536	70304
9	3	1	91296	73984
10	1	1	59616	30144

Computer packages like Mathematica [13] and Maple [14] contain functions that are able to calculate $y^x \bmod z$. The above algorithm shows, however, that these calculations can be done on paper, without spending more than a few minutes. Students experience satisfaction if they are able to find on their own how such functions work. Moreover, the algorithm can easily be implemented with a spreadsheet program or a scientific calculator. This implementation is part of the assignment. An Excel file is, as an example, available on the journal's website.

Once the students have implemented the algorithm, they can use it to explore properties of $y^x \bmod z$. For example, they can study the pseudo-randomness generated by the function $f(x) = (y^x \bmod z)/z$ by applying their statistical toolbox. Rigorous conditions on y and z for this randomness can be found in [9]. Or, alternatively, they can study the cyclic behaviour of the function $f(x) = y^x \bmod z$. Such exercises can stimulate students to practice experimental mathematics [15]. This is in contrast to exercises where students verify what they have already learnt [16].

5. Cycle length

Table 4 displays the last two digits of y^x for $1 \le y \le 15$ and $1 \le x \le x_2$, where $x_2 = \min\{x \ge 2 \mid \exists\, x_1 : 1 \le x_1 < x \text{ and } y^x \bmod 100 = y^{x_1} \bmod 100\}$ depends on y,

Table 4. The last two digits of y^x for $1 \le y \le 15$.

x \ y	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
2	01	04	09	16	25	36	49	64	81	00	21	44	69	96	25
3		08	27	64	25	16	43	12	29	00	31	28	97	44	75
4		16	81	56		96	01	96	61		41	36	61	16	25
5		32	43	24		76	07	68	49		51	32	93	24	
6		64	29	96		56		44	41		61	84	09	36	
7		28	87	84		36		52	69		71	08	17	04	
8		56	61	36				16	21		81	96	21	56	
9		12	83	44				28	89		91	52	73	84	
10		24	49	76				24	01		01	24	49	76	
11		48	47	04				92	09		11	88	37	64	
12		96	41					36				56	81	96	
13		92	23					88				72	53		
14		84	69					04				64	89		
15		68	07					32				68	57		
16		36	21					56				16	41		
17		72	63					48				92	33		
18		44	89					84				04	29		
19		88	67					72				48	77		
20		76	01					76				76	01		
21		52	03					08				12	13		
22		04													

as does x_1. The existence of x_1 and x_2 is guaranteed by the pigeon hole principle.[2] For example, if $y = 3$, then $x_1 = 1$ and $x_2 = 21$, because 1 and 21 are the smallest distinct exponents of 3 such that 3^1 and 3^{21} have the same last two digits. The pattern of the last two digits of y^x for $x \ge x_2$ is identical to the pattern of the last two digits of y^x for $x \ge x_1$. This follows from (3.1), since

$$\begin{aligned} y^{x_2+x} \bmod 100 &= ((y^{x_2} \bmod 100)(y^x \bmod 100)) \bmod 100 \\ &= ((y^{x_1} \bmod 100)(y^x \bmod 100)) \bmod 100 \\ &= y^{x_1+x} \bmod 100. \end{aligned}$$

Hence, $d = x_2 - x_1$ is the period of the function $f(x) = y^x \bmod 100$, defined for $x \ge x_1$. Table 4 shows that $d = 1$ for $y = 1$, 5, and 10; $d = 2$ for $y = 15$; $d = 4$ for $y = 7$; $d = 5$ for $y = 6$; $d = 10$ for $y = 4$, 9, 11, and 14; and $d = 20$ for $y = 2$, 3, 8, 12, and 13. All these values of d are divisors of 20 (notation: $d \mid 20$). Notice that $y^d \bmod 100 = 1$ for $y = 1$, 3, 7, 9, 11, and 13, which are the values of y in Table 4 that are relatively prime with respect to $z = 100$, i.e. for which $\gcd(y, 100) = 1$. We also see that 1 and 2 are the only values for x_1 in Table 4.

Most of the above remarks hold for general z, with x_1 and x_2 depending on both y and z. If $\gcd(y, z) = 1$, then the equation $y^{x_1} \bmod z = y^{x_2} \bmod z$ can be reduced

[2]At the International Mathematical Olympiad of 1978, the participants were asked to determine x_1 and x_2 for the last three digits of 1978^x; see [1].

to $y^d \bmod z = 1$. In this case, the exponent d is the smallest $x \in \mathbb{N}$ that solves the equation $y^x \bmod z = 1$ and is called the order of y modulo z; see e.g. [5].

The aim of the present section is to find an upper bound for the periods d in the case $z = 10^m$, but the major part of the following discussion is also valid for other values of z. Our discussion will be based on properties of Euler's totient function and of Carmichael's function. The encyclopaedic volumes [10, 11] contain an abundance of results about the Euler function, but without any proof, and [11] provides sufficient information about the Carmichael function.

5.1. **Euler's totient function.** Euler's totient function is defined by $\phi(z) = \#\{y \mid 1 \leq y \leq z \text{ and } \gcd(y, z) = 1\}$. The first six values of $\phi(z)$ are $\phi(1) = \#\{1\} = 1$, $\phi(2) = \#\{1\} = 1$, $\phi(3) = \#\{1, 2\} = 2$, $\phi(4) = \#\{1, 3\} = 2$, $\phi(5) = \#\{1, 2, 3, 4\} = 4$, and $\phi(6) = \#\{1, 5\} = 2$. Euler's function is multiplicative in the sence that $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$ if $\gcd(z_1, z_2) = 1$; see e.g. [5]. For example, $\phi(12) = \phi(3)\phi(4) = 4$, but $\phi(12) \neq \phi(2)\phi(6) = 2$.

Let p be a prime number, i.e. $p \in \{2, 3, 5, 7, 11, \ldots\}$. All positive integers y that are less than or equal to p^k, with $k \geq 1$, and satisfy $\gcd(y, p) \neq 1$ are given by $y = p, 2p, \ldots, p^{k-1}p$. Therefore, $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$. The Fundamental Theorem of Arithmetic asserts that every $z \in \mathbb{N}$ has a unique prime factorisation, i.e. $z = p_1^{k_1} \cdots p_n^{k_n}$; see e.g. [5]. Hence, if the factorisation of z is known, then $\phi(z)$ can be calculated with

$$\phi\left(\prod_{i=1}^{n} p_i^{k_i}\right) = \prod_{i=1}^{n} p_i^{k_i - 1}(p_i - 1). \tag{5.1}$$

It follows from (5.1) that $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)\gcd(z_1, z_2)/\phi(\gcd(z_1, z_2))$, but this property is not used in the present paper.

For our purpose, it is important to state Euler's theorem, which is famous in Number Theory (see e.g. [5]):

$$y^{\phi(z)} \bmod z = 1 \quad \text{if} \quad \gcd(y, z) = 1. \tag{5.2}$$

From (3.1) and (5.2) immediately follows that $y^{x+\phi(z)} \bmod z = y^x \bmod z$ if $\gcd(y, z) = 1$. Hence, whenever y and z are coprime, the period d of the function $f(x) = y^x \bmod z$ satisfies $d \leq \phi(z)$. It is known that d divides $\phi(z)$ (notation: $d \mid \phi(z)$). If $d = \phi(z)$, then y is said to be a primitive root modulo z. The only values of z that have a primitive root are $z = 2$, 4, p^k, and $2p^k$, with p an odd prime.

The condition $\gcd(y, z) = 1$ in (5.2) is a nuisance, that can be avoided by using the following generalisation of Euler's theorem:

$$y^{z-\phi(z)} \bmod z = y^z \bmod z \qquad \text{for all } y, z \in \mathbb{N}. \tag{5.3}$$

A nice proof of (5.3) can be found in [17], but the result is older; see the bibliographical remarks in [17, 11, 18]. In fact, (5.3) is stated in [18] as a corollary of two theorems that are formulated in subsection 5.2. The formulation of an other, more useful corollary in [18] is given next: If $z = p_1^{k_1} \cdots p_n^{k_n}$ is the prime factorisation of z and $N(z) = \max\{k_1, \ldots, k_n\}$ the largest exponent in the prime factorisation of z, then

$$y^{N(z)+\phi(z)} \bmod z = y^{N(z)} \bmod z \qquad \text{for all } y, z \in \mathbb{N}. \tag{5.4}$$

Due to (3.1), $y^{x+\phi(z)} \bmod z = y^x \bmod z$ for all $x \geq N(z)$. Thus, $N(z)$ is an upper bound for the onset x_1 of the periodic behaviour of $f(x) = y^x \bmod z$ and $\phi(z)$ is an upper bound for the period d of $f(x)$.

Specialising to the case $z = 10^m = 2^m 5^m$, we have $\phi(10^m) = 2^{m-1}(2-1)5^{m-1}(5-1)$, due to (5.1), and $N(10^m) = m$. We can therefore conclude that *the cycle length of the last m digits of y^x is at most $\phi(10^m) = 4 \times 10^{m-1}$ and that the first cycle starts at or before $N(10^m) = m$.* For example, if $m = 2$ (cf. Table 4), then $\phi(100) = 40$ and $N(100) = 2$. However, since $z = 10^m$ only has a primitive root if $m = 1$, an improved upper bound for the cycle length should be found in case $m \geq 2$.

5.2. **Carmichael function.** More than a century ago, Carmichael [12] introduced a function by[3]

$$\lambda(p^k) = \begin{cases} \phi(p^k) & \text{if } p \text{ is an odd prime and } k \geq 0, \\ \phi(2^k) & \text{if } k = 0, 1, 2, \\ \frac{1}{2}\phi(2^k) & \text{if } k \geq 3, \end{cases} \tag{5.5}$$

and

$$\lambda\left(\prod_{i=1}^{n} p_i^{k_i}\right) = \operatorname{lcm}\left(\lambda(p_1^{k_1}), \ldots, \lambda(p_n^{k_n})\right), \tag{5.6}$$

where $p_1, \ldots, p_n$ are different primes. It follows from (5.5) and (5.6) that $\lambda(z) \mid \phi(z)$ and

$$\lambda(\operatorname{lcm}(z_1, z_2)) = \operatorname{lcm}(\lambda(z_1), \lambda(z_2)). \tag{5.7}$$

Carmichael proved that $y^{\lambda(z)} \bmod z = 1$ for all positive integers y satisfying $\gcd(y, z) = 1$. Moreover, he showed that for each z there exists a y such that $\gcd(y, z) = 1$ and $x = \lambda(z)$ is the smallest solution of $y^x \bmod z = 1$; in this case, y is called a primitive λ-root modulo z. These properties suggest that the upper bound of subsection 5.1 can be improved, unless there exists a primitive (ϕ-)root modulo z. However, we experience the condition $\gcd(y, z) = 1$ as a burden, as we did in section 5.1.

The best description of our observations in Table 4 is provided by Theorems 1 and 2 of [18]. Theorem 1 in [18] states that

$$y^{N(z)+\lambda(z)} \bmod z = y^{N(z)} \bmod z \qquad \text{for all } y, z \in \mathbb{N}. \tag{5.8}$$

From (3.1) and (5.8) immediately follows that $y^{x+\lambda(z)} \bmod z = y^x \bmod z$ for all $x, y, z \in \mathbb{N}$, with $x \geq N(z)$. Theorem 2 in [18] implies that (5.8) can not be improved. It says that, if $x', x'' \in \mathbb{N}$ and $x' < x''$, then $y^{x'} \bmod z = y^{x''} \bmod z$ for *all* $y \in \mathbb{N}$ if and only if $x' \geq N(z)$ and $\lambda(z) \mid x'' - x'$.

For $z = 10^m$, we have $\lambda(10^m) = \lambda(\operatorname{lcm}(2^m, 5^m)) = \operatorname{lcm}(\lambda(2^m), \lambda(5^m))$, where the last equality uses (5.7). By invoking (5.6), we find that

$$\lambda(10^m) = \begin{cases} 4 \times 5^{m-1} & \text{if } m \leq 3, \\ \frac{1}{2} \times 10^{m-1} & \text{if } m \geq 4. \end{cases} \tag{5.9}$$

Table 5 compares the values of $\phi(10^m)$ and $\lambda(10^m)$ for $1 \leq m \leq 6$ and shows that the upper bound (5.9) is a significant improvement for $m \geq 2$. By the properties of $\lambda(z)$, the upper bound $\lambda(z)$ is actually attained; cf. Table 4, where $d = \lambda(100) = 20$ for $y = 2$, 3, 8, 12, and 13.

[3]Carmichael's function should not be confused with Carmichael numbers $z \in \mathbb{N}$, which are composite numbers with the property that $y^{z-1} \equiv 1 \pmod{z}$ for all $y \in \mathbb{Z}$ with $\gcd(y, z) = 1$; see e.g. [5].

Table 5. Comparison of $\phi(10^m)$ and $\lambda(10^m)$.

m	$\phi(10^m)$	$\lambda(10^m)$
1	4	4
2	40	20
3	400	100
4	4000	500
5	40000	5000
6	400000	50000

References

[1] http://www.artofproblemsolving.com

[2] Andreescu T, Andrica D, Feng Z. 100 Number Theory Problems – From the Training of the USA IMO Team. Birkhäuser, Boston; 2007.

[3] Rassias MT. Problem-Solving and Selected Topics in Number Theory – In the Spirit of the Mathematical Olympiads. Springer, New York; 2011.

[4] Teleuca M. Zsigmondy's theorem and its applications in contest problems. International Journal of Mathematical Education in Science and Technology 2013; 44 (3): 443–551.

[5] Stein W. Elementary Number Theory: Primes, Congruences, and Secrets – A Computational Approach. Undergraduate Texts in Mathematics, Springer, New York; 2009.

[6] Baldoni MW, Ciliberto C, Piacentini Catteneo GM. Elementary Number Theory, Cryptography and Codes. Universitext, Springer, Berlin; 2009.

[7] Hoffstein J, Pipher J, Silverman JH. An Introduction to Mathematical Cryptography. Undergraduate Texts in Mathematics, Springer, New York; 2008.

[8] Asmussen S, Glynn PW. Stochastic Simulation – Algorithms and Analysis. Stochastic Modelling and Applied Probability, Volume 57, Springer, New York; 2007.

[9] Friedlander JB, Pomerance C, Shparlinski IE. Period of the power generator and small values of Carmichael's function. Mathematics of Computation 2001; 70 (236): 1591–1605.

[10] Sándor J, Mitrimović DS, Crstici B. Handbook of Number Theory I. 2nd printing, Springer, Dordrecht; 2006.

[11] Sándor J, Crstici B. Handbook of Number Theory II. Kluwer Academic Publishers, Dordrecht; 2004.

[12] Carmichael RD. Note on a new number theory function. Bulletin of the American Mathematical Society 1910; 16 (5): 232–238.

[13] http://reference.wolfram.com/mathematica/ref/PowerMod.html

[14] http://www.maplesoft.com/support/help/Maple/view.aspx?path=mod

[15] Ruiz Jiménez BC, Ruiz Muñoz M. From recreational mathematics to recreational programming, and back. International Journal of Mathematical Education in Science and Technology 2011; 42 (6): 775–787.

[16] Cheung YL. Learning number theory with computer algebra system. International Journal of Mathematical Education in Science Technology 1996; 27 (3): 379–385.

[17] Alzer H. The Euler-Fermat theorem. International Journal of Mathematical Education in Science and Technology 1987; 18 (4): 635–636.

[18] Singmaster D. A maximal generalization of Fermat's theorem. Mathematics Magazine 1966; 39 (2): 103–107.

KU Leuven
Faculty of Economics and Business
Centre for Information Management, Modelling and Simulation
Warmoesberg 26, 1000 Brussels, Belgium
E-mail address: edward.omey@kuleuven.be, stefan.vangulck@kuleuven.be